Command and Control Division
Maritime and Expeditionary Command and Control
Capability-Based In-Service Systems Engineering Activity; Development, Security, and Operations

1.0 SCOPE

This statement of work (SOW) includes Command, Control, Communications, Computers, and Intelligence (C4I) software development, security, operations, maintenance, and support services in support of Command and Control Division, Naval Information Warfare Command (NIWC) Pacific.

Services and deliverables under this SOW support information technology both ashore and afloat. Services and deliverables under this SOW may occur within the Continental United States (CONUS) and Outside the Continental United States (OCONUS).

This is a severable, level-of-effort type contract.

2.0 BACKGROUND

The Command and Control (C2) Systems Division (Code 532) within NIWC Pacific provides systems engineering, software development, maintenance, integration, test, and life-cycle support for a wide range of Navy, Joint, and National C4I systems. These systems serve to consolidate Command, Control, Intelligence, Imagery, Planning, Coordination and Logistic capabilities to provide an integrated C4I capability to the warfighter. Variants of these systems are installed in Navy, Joint, and National Command Centers both ashore and afloat.

NIWC Pacific intends to transition some of its software products from a Capability-Based-In Service Engineering Activity model to a Development, Security, and Operations (DevSecOps) model of service. As such, the contractor must be able to conduct software activities using both methodologies and practices.

3.0 TECHNICAL REQUIREMENTS

3.1 Capability-Based In-Service Systems Engineering Activity (CB-ISEA) Services

There are four core services (pillars) and 11 sub-services associated with the Mar/EXP C2 CB-ISEA. Some of the work at the sub-service level for the CB-ISEA work is executed out of NIWC Atlantic and is not a part of this SOW. CB-ISEA services are organized as shown in Figure 1.

The CB-ISEA is responsible for executing the services as outlined in the Naval Information Warfare Center (NIWC) Atlantic and Pacific Capability-Based (CB-ISEA) service catalog. These services are performed onboard naval vessels and shore facilities, remotely, and within cloud-hosted infrastructure.

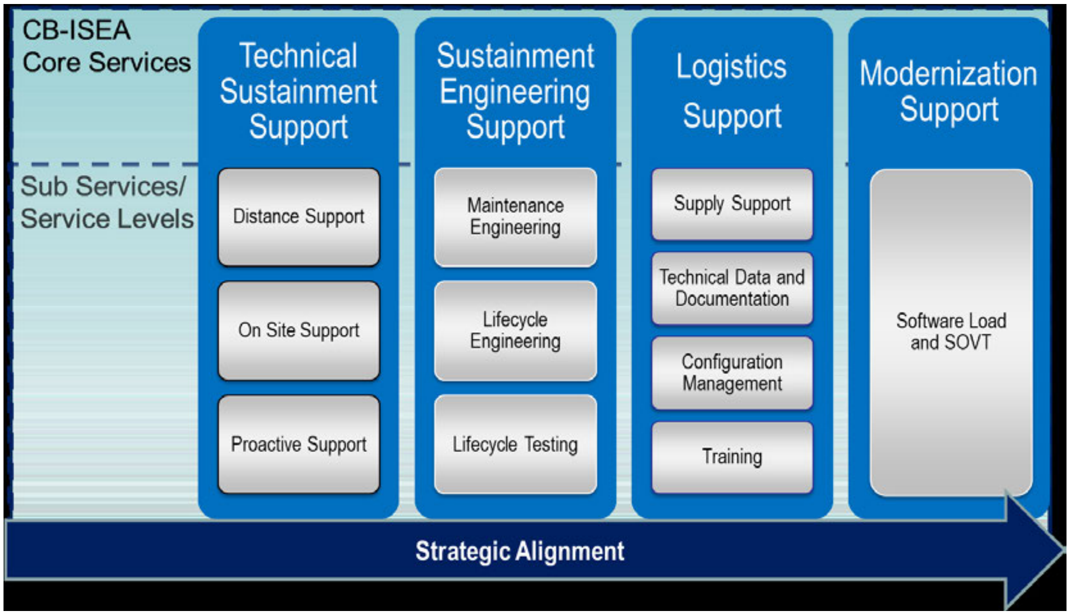

Figure 1. Capability-Based In-Service Systems Engineering Activity

3.1.1 Technical Sustainment Support

Technical Sustainment support includes Help Desk Support and system upgrades support including associated system engineering support for operation, maintenance upgrade, Board of Inspection Survey (INSURV), System Operation Test (SOT), Deploying Group System Integration Team (DGSIT), Ships Restricted Availability (SRA), Combat Systems Ship Qualification Trials (CSSQT) and system administration for C4I system variants. The contractor shall provide operational support for the designated C2/C4I systems, with On-Board Technical Assistance (OBTA) and on-site for NIWC Pac Tier 2 and Tier 3 assists. Tier 2 support is an escalation of the incident/service request (SR) from Tier 1 and provides advanced technical expertise to the customer. Tier 3 provides support or information on issues including hardware or software, and usually involves certified systems engineers or additional levels of specialized or authoritative expertise not available at Tier 1 and 2. Both Tier 2 and Tier 3 resolutions will be documented for visibility and tracking.

This effort will include installations, integration, System Operational Verification Testing (SOVT) and integration of C4I components at operational sites. Support also includes exercise support and Post Installation Training (PIT).

3.1.1.1 Distant Support

Distant support includes Tier 2 Help Desk Support and Tier 3 Help Desk Support performed onsite or via approved telework locations at NIWC Pacific, located in San Diego.

3.1.1.2 Onsite Support

Onsite support includes CASREP response either ashore or afloat that is performed onsite at the customer/unit location. Execution may be required with a minimum 24-hour notification from the Government and may require extended duration. Planned support is 16-hour shifts while underway, along with 10-hour shifts (8-hour shifts for INSURV) while in port. If not already accounted for in the job estimation, extended working hours must be coordinated with the Contracting Officer's Representative prior to execution. Funding shall be tracked on a per-effort basis. Status reports shall be submitted on a daily basis. Trip reports and Technical Assist Visit Reports shall be submitted upon completion of an effort.

3.1.2 Sustainment Engineering (SE)

Sustainment Engineering (SE) spans technical tasks including engineering, logistics investigations and analyses to ensure continued operation and maintenance of a fielded system. SE provides support to fleet customers by providing timely data analysis, development, and implementation of engineering changes and tech advisories through approved enterprise processes relative to customer's service request. The service has a critical success factor to robustly deliver baseline changes through three subservices to include Maintenance Engineering, Lifecycle Engineering, and Sustainment Engineering.

Although Lifecycle Testing is a part of the SE ISEA pillar, other than providing necessary SE support to/for Lifecycle Testing, Lifecycle Testing is not a part of this SOW. To enforce the independence of Lifecycle Testing, the testing tasking work will be a different competitive action.

3.1.2.1 Maintenance Engineering

The Maintenance Engineering sub-service develops corrective and preventative maintenance documentation and is an active participant in Engineering Change Solutions to improve Mar C2 CB-ISEA systems' overall maintainability.

3.1.2.2 Lifecycle Engineering

The Lifecycle Engineering sub-service provides the analysis required to identify critical issues and resolutions in a timely fashion, in order to maintain and support Mar C2 CB-ISEA systems throughout the lifecycle. The overall goal of the service is to improve Mar C2 CB-ISEA systems' readiness through the improvement of Reliability, Maintainability, and Availability (RMA).

3.1.2.2.1 Lifecycle Engineering - System Integration

As part of Lifecycle Engineering, the contractor shall perform systems integration engineering to technically plan for, implement, and gain acceptance of C2 and C4I components and networks integrated into Navy, Joint, National, and Foreign Military C2/C4I systems.

3.1.2.2.2 Lifecycle Engineering - Software Development & Maintenance

The Government has developed multiple fielded applications that support C2 systems. The contractor shall maintain and support these production applications, which will include updating and upgrading system components to align with technology advances, security updates and/or hardware upgrades.

3.1.2.3 Sustainment Engineering - Cyber Engineering (CE)

Cybersecurity Engineering (CE) services supports all Mar C2 CB-ISEA capabilities. CE is a technical task, with all contractors supporting the CE team should have technical backgrounds and education/certifications of those working on lifecycle engineering and integration tasks.

3.1.3 Logistics Support

3.1.3.1 Technical Data and Documentation

The contractor shall develop system and user documentation for both existing and newly deployed application software. The contractor shall provide the following documentation for each application:

a) System Documentation, to include Assured Compliance Assessment Solution (ACAS) scanning documentation
b) Training Documentation
c) User Documentation, to include system user and system administration guides

3.1.3.2 Training

The contractor shall support Integrated Learning Environment (ILE) updates for legacy capabilities in sustainment. The contractor shall provide technical expertise in all phases of training and exercise support ashore and afloat to include planning, analysis, design, development, implementation, evaluation, life cycle maintenance, and training equipment support as identified in and in accordance with NAVEDTRA 136 and its cited publications. Support includes preparation of or updating training materials and performing training and indoctrination at NIWC Pacific and operational sites.

3.1.3.3 Infrastructure, Lab and Operations Support

Infrastructure Modernization, Maintenance, and Support provides engineering and technical support services to all projects. The work will include designing, securing, implementing, maintaining, updating, and decommissioning classified and unclassified Information Technology (IT) and facilities. This may include individual hardware and software components in stand-alone systems to larger computing environments such as system-of-systems, enclaves, and networks. Facilities primarily consist of classified and unclassified laboratories, storage rooms, storage containers, and staff offices. The work will also include those hardware and software components and systems needed to support Shipbuilding and Conversion, Navy (SCN). Services and deliverables under this requirement support IT both ashore and afloat. Services and deliverables under this requirement may occur within the Continental United States (CONUS) and Outside the Continental United States (OCONUS).

3.1.4 Modernization Support

The contractor shall perform C4I installations, software-only or with associated hardware, at various shipboard and shore sites. Software versions will be determined at the time of installation to align with what is currently authorized for fielding.

Execution may be required with a minimum 24-hour notification from the Government and may require extended duration. Support shall be executed in 10-hour shifts from Monday through Saturday. Extended working hours must be coordinated with the COR or ACOR prior to execution.

Funding shall be tracked on a per-site/job basis. Status reports shall be submitted on a daily basis. Trip reports shall be submitted upon completion of an effort.

3.2 Development, Security, and Operations (DEVSECOPS)

DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted to the left through automated unit, functional, integration, and security testing - this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously. Figure 2 offers a notional DevSecOps software lifecycle established through Overmatch Software Armory's (OSA) factory.

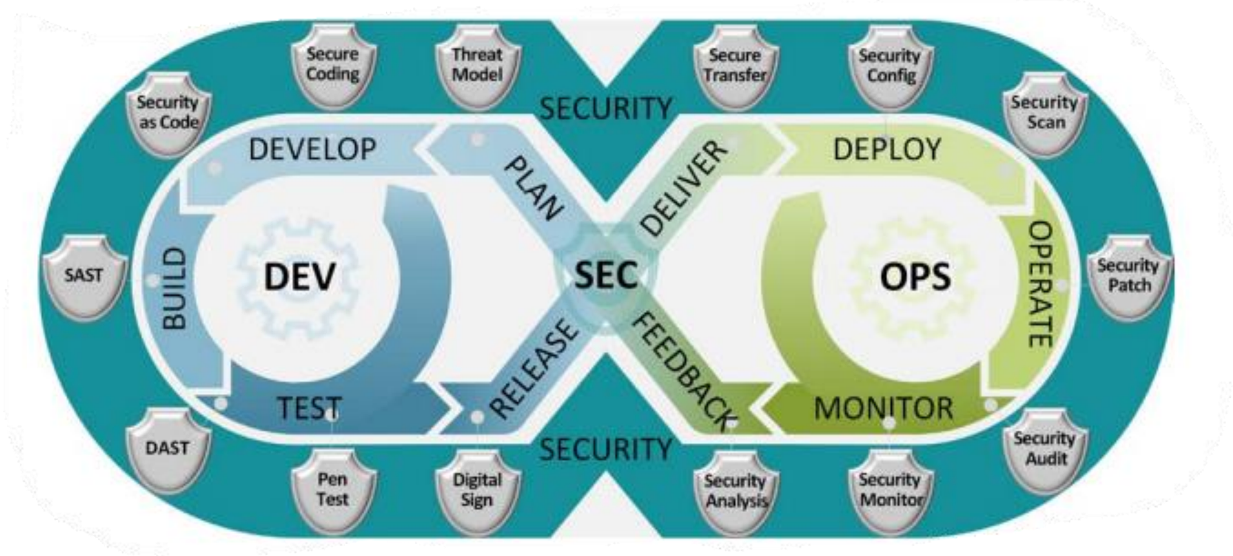

Figure 2. DevSecOps Software Lifecycle

(b)4 [redacted]

(b)4

[redacted]

3.2.1 Battle Management Aid DevSecOps Product Team

Cross-functional product teams shall be required to re-architect and re-platform legacy software products. This effort shall be in accordance with DevSecOps software practices outlined in the DoD Enterprise DevSecOps Reference Design. The effort shall occur within OSA's factory, processes, and technologies. An example cross-functional product team is listed in Table 2.

Table 2. Example Battle Management Aid DevSecOps Product Team

Product Owner	Design Lead
Software Development Lead	Designer
Software Developer	Tester
Cybersecurity Specialist	Systems Administrator

3.2.2 Battle Management Aid Support Team

Battle Management Aid product teams external to NIWC Pacific (e.g. products from the Office of Naval Research) will require technical, installation, user experience, testing, and configuration management support as they re-platform and refactor their applications to receive approval within the Overmatch Software Armory.

3.2.3 Continuous Integration/Continuous Delivery Software Pipeline Team

Functional support teams shall be required to support a fully functional cloud-based software factory. As seen in Figure 3, functional support teams can expect to interact with all aspects of the DevSecOps software factory.

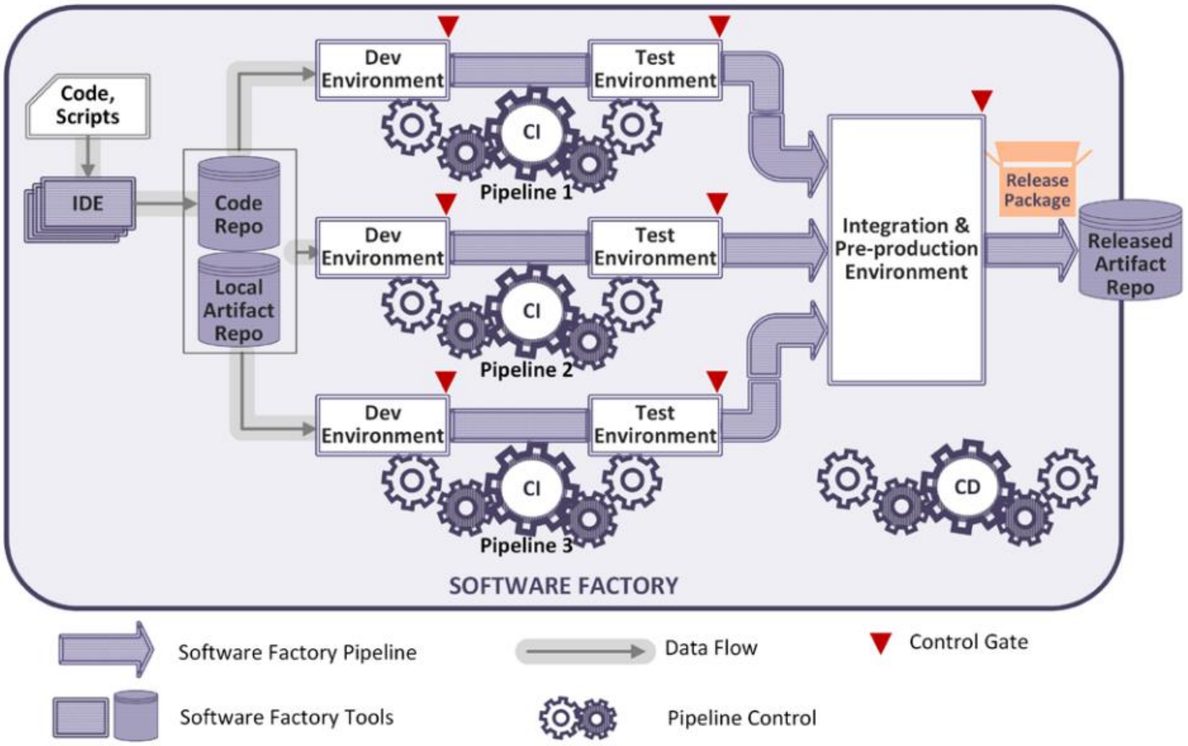

Figure 3. DevSecOps Software Factory

(b)4

[redacted]

4.1 <u>Transition Out</u>

The contractor shall provide support for an efficient and effective ten (10) business day transition of contract activities to the successor contractor. The transition shall occur within the period of performance of this task order. The contractor shall continue to execute all tasks under this SOW until successful turnover and transition with the successor contractors are completed and approved by the Contracting Officer's Representative (COR).

As completion of this contract approaches, contractor manpower and level of effort shall be reduced and ultimately phased out as the successor contractors develop the ability to seamlessly take over and perform assigned tasks. The contractor shall provide support for the programs described under the cognizance of NIWC Pacific.

5.0 GOVERNMENT FURNISHED EQUIPMENT/INFORMATION (GFE/GFI)

None anticipated at this time.

6.0 OTHER

6.1 Security

Work performed and work products are all at the SECRET level and below. Some efforts may require personnel to be cleared to the TOP SECRET/SCI level because on-site work performed will be predominantly in active SCIF areas. The contractor will not be producing any TS/SCI level deliverables. All other individuals supporting this task must be cleared to the SECRET level because on-site work will require access to SECRET information. Contractor personnel assigned to this effort who require access to SCI spaces must possess a current Single Scope Background Investigation (SSBI) with Intelligence Community (IC) Directive 704 (ICD 704) eligibility (which replaced Director of Central Intelligence Directive (DCID) 684 eligibility).

The contractor will require access to Communications Security (COMSEC) and the Secure Internet Protocol Router Network (SIPRNet). The contractor shall receive North Atlantic Treaty Organization (NATO) awareness brief and complete the derivative classification training prior to being granted access to SIPRNet; training is provided by the facility security officer.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to Commanding Officer, Attn: Foreign Travel Team, Naval Information Warfare Center, Pacific, 53560 Hull Street, Building 27, 2nd Floor -Room 206, San Diego, CA 92152 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 30 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/ Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure. Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is ssc_fortrav@navy.mil. Forward a copy of the training certificate to the previous email address or fax to (619) 553-6863. SERE 100.1 Level A Code of Conduct training is also required prior to OConus travel for all personnel. SERE 100.1 Level A training can be accessed at https://wwwa.nko.navy.mil. Other specialized training for specific locations may also be required contact the NIWC Pacific foreign travel team. Program (STEP). When you sign up, you will automatically receive the most current information the State Department compiles about your destination country. You will also receive updates, including Travel Warnings and Travel Alerts. Sign up is one-time only, after you have established your STEP account, you can easily add official or personal travel to anywhere in the world, not just EUCOM. http://travel.state.gov/content/passports/en/go/step.html

Applicable documents are as follows SECNAV Manual 5510.30 (Series), Department of Navy Personnel Security Program, SECNAV Manual 5510.36 (Series), Department of Navy Information Security Program, DOD 5200.01 Volumes 1 through 4 (Series), DOD Security Program, and DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM).

6.2 Operations Security (OPSEC)

OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or Critical Program Information, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

Applicable documents are as follows OPNAVINST F3300.53C (Series), Navy Antiterrorism Program, National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298, DOD 5205.02 (Series), DOD Operations Security (OPSEC) Program, OPNAVINST 3432.1 (Series), DON Operations Security, and SPAWARINST 3432.1 (Series), Operations Security Policy.

6.3 Places of Performance

It is anticipated that 90% of the tasking under this contract will be performed at Government facilities and 10% at contractor facilities.

6.4 Travel

It is anticipated that CONUS and OCONUS travel will be required under this contract.

6.5 Lab Open and Close Security

The contractor shall be required to securely open and close designated NIWC Pacific Code 532 SECRET level lab facilities in accordance with NIWC Pacific Instructions (SSCPACINST 5500.1B, Security Manual (7 JUN 10)) and 532 Lab Manager's security policies (Maritime Global Command and Control System (GCCS) Family of Systems (FoS) (MGF) Security Manual, Version 2.1, dated April 17, 2012). The contractor shall coordinate with the 532 Lab Manager in designating which contractor team members will be allowed opening and closing authority and to notify the Lab Manager when changes occur.

6.6 Cybersecurity Workforce Certification

Contractor personnel are required to meet NIWC PAC CSWF Program standards before arriving to the worksite in order to gain privileged access (IAT 1/2/3) on DoD any computer systems.

- For specifics on security baseline certifications, refer to https://public.cyber.mil/cw/cwmp/dod-approved-8570-baseline-certifications/

- For specifics on IAT Level functions refer to Chapter 3 of DoD 8570.01-M; https://public.cyber.mil/cw/cwmp/cwmp-faqs/#toggle-id-2

Additionally, Operating System (OS)/Computing Environment (CE) training or certification is required for the system(s) being accessed with privileged access. Any number of commercial and non-commercial training providers are available. The COR will address any specific questions concerning OS/CE venues.

7.0 FOREIGN TRAVEL

Contractor personnel are reminded of their obligation to safeguard the vital relationship our Nation has with Foreign Countries. This includes personal conduct while performing under the contract and on one’s personal time because, at all times, you are viewed by our partners as a representative of the United States, our Navy, and NAVWAR. Therefore, professional, courteous, and culturally aware conduct is necessary at all times. Inappropriate conduct, and especially intoxication and criminal behaviors, will not be tolerated. An all-too-common nexus for personnel misconduct while on travel is irresponsible consumption of alcohol. Intoxication increases your vulnerability to crime, injury, arrest, terrorism and espionage. While traveling on official business, representing and performing in support of NAVWAR’s mission, all personnel, including military, civilian and contractors, are expected to act in a professional and responsible manner. In order to promote effective relationships with business partners and allied nations, it is incumbent on contractor personnel to follow local laws and employ courteous and culturally aware behavior. Inappropriate conduct may jeopardize important relationships for the United States Navy, NAVWAR, NIWC Pacific and NIWC Atlantic, and will not be tolerated.

8.0 APPLICABLE DOCUMENTS

The following documents, inclusive of references, are applicable to this SOW:

- Chief of Naval Operations Cybersecurity Safety (CYBERSAFE) Program, OPNAVINST 5239.4
- Classified Material Control Center (CMCC) Handbook
- Communications Security Material System Material and Equipment Guidance - NIWC PACIFIC INSTRUCTION 2280.2C
- DoD 8570.01-M, Information Assurance Workforce Improvement Program, Change 4, dated November 10, 2015
- Cybersecurity Policy - NIWC PACIFIC INSTRUCTION 5239.4
    - Includes Cybersecurity Workforce
- DoD Enterprise DevSecOps Reference Design, v1.0, 12 August 2019
- DoD Instruction (DoDI) 8500.01, Cybersecurity
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- Foreign Travel Program - NIWC PACIFIC INSTRUCTION 4650.3B

- Guide for Conducting Risk Assessments, NIST Special Publication 800-30
- Medical Screening for U.S. Government Civilian Employees, Contractor Employees, Guests, and Visitors Prior to Embarking Fleet Units - COMUSFLTFORCOM/COMPACFLT INSTRUCTION 6320.3B
- Maritime Global Command and Control System (GCCS) Family of Systems (FoS) (MGF) Security Manual, Version 2.1, dated April 17, 2012
- Navy Authorizing Official (NAO) Guidance Memorandum; Approval of Changes to Risk Management Framework (RMF) Authorized Systems, Networks or Applications, FCC MEMO 5239, Ser. NAO/0557
- Navy Ports, Protocols, and Services Management (PPSM) Manual
- Navy Qualified Validator Fact Sheet
- Navy Qualified Validator, SPAWAR MEMO 5239, Ser. 5.0/362
- Navy Security Control Assessor (SCA) Risk Management Framework (RMF) Assessment & Authorization (A&A) Testing Guidance
- Policies and Procedures on Shipments - NIWC PACIFIC INSTRUCTION 4610.1C
- Policy and Procedures for Control and Operation of Secure Telephone Equipment and the Associated KEYMAT - NIWC PACIFIC INSTRUCTION 2280.1D
- Release of Classified and Unclassified General and Technical Information - NIWC PACIFIC INSTRUCTION 5720.1B
- Research, Development, Test, and Evaluation Network Governance, Operation, and Usage Policy - NIWC PACIFIC INSTRUCTION 5239.6
- Risk Management Framework for Information Systems and Organizations, NIST Special Publication 800-37
- Safety and Occupational Health Program - NIWC PACIFIC INSTRUCTION 5100.5E
- Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53
- Security Manual - NIWC PACIFIC INSTRUCTION 5500.1C
- Security Categorization and Control Selection for National Security Systems, Committee on National Security Systems Instruction (CNSSI) No. 1253
- Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199
- Standard Operating Procedure (SOP), NIWC Pacific RDT&E Limited Integrated Test Event
- United States Navy Information Assurance Technical Authority (IA TA) Information Security Continuous Monitoring (ISCM) Standard, STD-ISCM-005R0
- United States Navy Information Security Continuous Monitoring Program, OPNAV MEMO 5000, Ser. N2N6/17U119178
- Updated Risk Management Framework System Security Categorization Approval Process, OPNAV MEMO 5000, Ser. N2N6G/7U120115
- US Navy Risk Management Framework Implementation Strategy, OPNAV MEMO 8510, Ser. N2N6/7U120027
- Volume I: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, NIST Special Publication 800-60 Volume I
- Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, NIST Special Publication 800-60 Volume II

- Weight Handling Equipment and Rigging Gear Management - NIWC PACIFIC INSTRUCTION 11262.1F

9.0 FUNDING SOURCES

The below funding sources are applicable to all paragraphs of this SOW.

PMW-150
9.1 Global Command and Control System-Maritime (GCCS-M) (OMN)
9.2 Global Command and Control System-Maritime (GCCS-M) (OPN)
9.3 Global Command and Control System-Maritime (GCCS-M) (SCN)
9.4 Maritime Tactical Command and Control (MTC2) (RDTE)
9.5 Maritime Tactical Command and Control (MTC2) (OMN)
9.6 Maritime Tactical Command and Control (MTC2) (SCN)
9.7 Naval Air Operations Command and Control (NAOC2) with sub capabilities Theater Battle Management Core Systems (TBMCS), Joint Automated Deep Operations Coordination System (JADOCS), and Kessel Run (RDTE)
9.8 Naval Air Operations Command and Control (NAOC2) with sub capabilities Theater Battle Management Core Systems (TBMCS), Joint Automated Deep Operations Coordination System (JADOCS), and Kessel Run (OMN)
9.9 Naval Air Operations Command and Control (NAOC2) with sub capabilities Theater Battle Management Core Systems (TBMCS), Joint Automated Deep Operations Coordination System (JADOCS), and Kessel Run (SCN)

PMA-280/281
9.10 Maritime Strike Tomahawk (MST) (RDTE)

MDA
9.11 Missile Defense Agency (MDA) (RDTE)

Field Installation, Engineering, and Logistics Division
9.12 IMO/Fleet Support (Service Center)

PEO IWS
9.13 PEO IWS (RDTE)

(End of SOW)